(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020030008453 A
(43)Date of publication of application: 29.01.2003

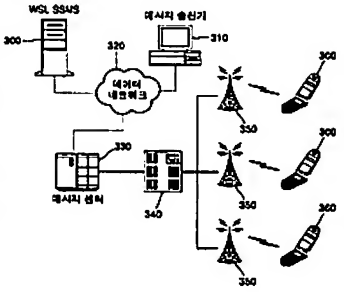
(21)Application number: 1020010043104
(22)Date of filing: 18.07.2001
(30)Priority: ..

(51)Int. Cl H04L 9/32

(71)Applicant: WIRELESS SECURITY LAB, INC.
(72)Inventor: KIM, GI TAE
LEE, IM JUN

(54) MUTUAL AUTHENTICATION AND SECURITY SERVICE METHOD USING USERS PASSWORD AT BIDIRECTIONAL SHORT MESSAGE SERVICE ON CDMA NETWORK

(57) Abstract:



PURPOSE: A mutual authentication and security service method using users password at bidirectional short message service on cdma network is provided to be capable of realizing a security-needed service on a wireless communication by providing a mutual authentication and security service at a bidirectional short message service. CONSTITUTION: A security short message service(SSMS) server(300) generates a temporary key using an identification number and a password of a user. The SSMS server(300) generates random numbers to be used when generating a section key, and encodes the temporary key to be transferred to a mobile terminal(360). A user of the mobile terminal(360) inputs own password to generate a temporary key. The user of the mobile terminal(360) decodes the temporary key to regenerate random numbers. The server(300) and the mobile terminal(360) generate secondary temporary keys using the regenerated random numbers respectively, and the secondary temporary keys are used for parameter encoding and decoding of a challenge-response protocol. A final section key is generated using two temporary keys and the second random numbers generated in the server(300). User data is encoded and decoded with the section key.

copyright KIPO 2003

Legal Status
Date of request for an examination (20010718)
Notification date of refusal decision (00000000)
Final disposal of an application (rejection)
Date of final disposal of an application (20030829)
Patent registration number ( )
Date of registration (00000000)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent ( )
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl. [7]
H04L 9/32

(11) 공개번호 특2003-0008453
(43) 공개일자 2003년01월29일

(21) 출원번호 10-2001-0043104
(22) 출원일자 2001년07월18일

(71) 출원인 주식회사 더블유에스랩
서울 강남구 역삼1동 628-6 서울빌딩 5층

(72) 발명자 김기태
서울특별시강남구삼성동106번지풍림아파트1508호
이임준
서울특별시동작구사당동1035-10

(74) 대리인 이영필
이해영

심사청구 : 있음

(54) CDMA네트워크 상의 양방향 단문메시지 서비스에서사용자 패스워드를 이용한 상호인증 및 보안서비스 방법

요약

본 발명은 CDMA상의 응용 서비스 중 양방향 단문 메시지 서비스에서 상호인증과 보안 서비스를 제공하여 무선상에서 보안이 필요한 서비스를 구현할 수 있도록 하는 통신프로토콜과 구현 알고리즘에 관한 것이다.

본 발명에 의한 양방향 단문메시지 서비스에서 사용자 패스워드를 이용한 상호인증 및 보안서비스 방법은 (a)사용자 식별번호와 패스워드를 가지고 임시키를 만들고, 세션키 생성에 사용될 난수를 발생시키고, 상기 난수를 임시키로 암호화하여 무선단말기에 전송하는 단계; (b)상기 무선단말기에 사용자의 패스워드를 입력하여 임시키를 생성한 다음 복호화하여 난수를 재생하는 단계; (c)상기 재생된 난수를 가지고 상기 서버와 상기 무선단말기는 각각 두 번째 임시키를 만드는 단계; (d)상기 두 임시키와 상기 서버에서 생성하는 두 번째 난수까지 포함하여 세션키를 생성하는 단계; 및 (e)상기 세션키를 이용하여 암호화 및 복호화하는 단계를 포함함을 특징으로 한다.

본 발명에 의하면, 기존의 보안성 없는 단문메시지 서비스로는 불가능했던 다양한 서비스들이 제공 가능해진다. 이는 기존의 무선 인터넷폰에서만 가능했던 서비스들을 기존의 구형단말기들에서도 가능하게 해준다.

대표도

도 4

명세서

도면의 간단한 설명

도 1은 종래의 단문메시지 서비스 구성도를 도시한 것이다.

도 2는 종래의 단문메시지 서비스에 대한 프로토콜 계층도를 도시한 것이다.

도 3은 본 발명에 의한 CDMA네트워크 상의 양방향 단문메시지 서비스에서 사용자 패스워드를 이용한 상호인증 및 보안서비스의 구성도를 도시한 것이다.

도 4는 본 발명에 의한 CDMA네트워크 상의 양방향 단문메시지 서비스에서 사용자 패스워드를 이용한 상호인증 및 보안서비스에 대한 프로토콜 계층도를 도시한 것이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 CDMA상의 응용 서비스 중 단문메시지 서비스에 관한 것으로, 특히 양방향 단문 메시지 서비스에서 상호인증과 보안 서비스를 제공하여 무선상에서 보안이 필요한 서비스를 구현할 수 있도록 하는 통신프로토콜과 구현 알고리즘에 관한 것이다.

종래의 단문메시지 서비스는 크게 단방향과 양방향으로 나누어져 있다. 이러한 단문메시지 서비스는 CDMA표준의 일부로서 현재 한국내 모든 이동전화 단말기는 단문메시지 서비스를 제공한다.

도 1은 종래의 단문메시지 서비스 구성을 도시한 것으로, 메시지 송신기(100), 메시지 센터(110), 데이터 네트워크(120), 셀룰라 스위치(130), 기지국(140) 및 이동통신단말기(150)로 이루어진다.

도 2는 종래의 단문메시지 서비스에 대한 프로토콜 계층도를 도시한 것이다.

단문메시지 서비스의 프로토콜은 크게 단문메시지 서비스 텔레서비스 계층, 단문 메시지 서비스 전송 계층 및 단문메시지 서비스 릴레이 계층의 3계층으로 이루어져 있다.

링크계층은 EIA/TIA/IS-95A를 사용하여 기지국(Base Station:140)과 연결하고 있다. 단문메시지 서비스 전송계층과 릴레이 계층은 실제 메시지 센터(110)와 단대단으로 연결될 필요는 없으나 단문메시지 서비스의 텔레서비스 계층은 메시지 센터(110)와 단대단으로 연결되어야 한다. 따라서 기지국(140)과 메시지 센터(110)와는 유선망으로 연결되어 전송계층까지는 EIA/TIA/IS-95A와 그 상위 단문메시지 서비스 전송계층과 릴레이 계층을 통해서 연결된다.

현재 단문메시지 서비스에서는 보안이 이루어지지 않고 있다. 이것은 단문메시지의 크기 때문으로써 상호인증을 위한 공개키 사용시 단문메시지 내에 충분한 정보를 넣을 수 없기 때문이다. 현재 국내에서 사용되고 있는 단문메시지 서비스의 경우 80바이트까지의 데이터를 지원하고 있다. 하지만 공개키 알고리즘은 이보다 훨씬 큰 데이터를 요구하고 있다.

예를 들어 디피헬만 공개키 알고리즘이나 RSA공개키 알고리즘의 경우 공개키의 크기가 최저 512비트, 보통은 1024비트가 일반적이다. 즉 공개키의 크기만 최저 64바이트, 보통 128바이트가 된다. 따라서 공개키 사용에 필수적인 인증서에 포함되는 CA의 공개키를 합치며 이미 80바이트 내에 공개키를 포함시킬 수 없다.

타원곡선 공개키 암호화 알고리즘은 128비트의 크기만으로 RSA의 1024비트 정도의 보안성을 제공하는 것으로 알려져 있다. 그러나 두 개의 공개키 크기만 32바이트를 차지하고 여타 파라미터들 역시 32바이트 이상되어 실제로 보낼 수 있는 데이터는 16바이트에 지나지 않는다. 또한 세션을 구성하기 위해서 프로토콜 자체적으로 페이로드가 발생하여 현실적으로 사용이 불가능하다.

발명이 이루고자 하는 기술적 과제

발명이 이루고자하는 기술적 과제는 양방향 단문 메시지 서비스에서 상호인증과 보안 서비스를 제공하여 무선통신 상에서 보안이 필요한 서비스를 구현할 수 있도록 하는 통신프로토콜을 제공함에 있다.

또한, 양방향 단문메시지 서비스를 이용한 무선뱅킹서비스 방법을 제공함에 있다.

발명의 구성 및 작용

상기 기술적 과제를 해결하기 위한 본 발명에 의한 양방향 단문메시지 서비스에서 사용자 패스워드를 이용한 상호인증 및 보안서비스 방법은 (a)사용자 식별번호와 패스워드를 가지고 임시키를 만들고, 세션키 생성에 사용된 난수를 발생시키고, 상기 난수를 임시키로 암호화하여 무선단말기에 전송하는 단계; (b)상기 무선단말기에 사용자의 패스워드를 입력하여 임시키를 생성한 다음 복호화하여 난수를 재생하는 단계; (c)상기 재생된 난수를 가지고 상기 서버와 상기 무선단말기는 각각 두 번째 임시키를 만드는 단계; (d)상기 두 임시키와 상기 서버에서 생성하는 두 번째 난수까지 포함하여 세션키를 생성하는 단계; 및 (e)상기 세션키를 이용하여 암호화 및 복호화하는 단계를 포함함을 특징으로 한다.

또한, 상기 세션키는 하나의 세션 또는 트랜잭션으로 제한되어 그 세션이 끝나거나 연결이 끊어지며 또 다른 세션키를 생성함을 특징으로 한다.

또한, 상기 세션키는 생성과정에서 두 개의 난수가 사용됨으로써 세션키의 난수성을 보장하고 있으며 Brute-Force 공격과 오프라인 Dictionary 공격을 방지함을 특징으로 한다.

상기 다른 기술적 과제를 해결하기 위한 본 발명에 의한 양방향 단문메시지 서비스를 이용한 무선뱅킹서비스 방법은 (a)이동통신 사업자의 단문 메시지 센터와 은행의 보안 단문 메시지 서버를 연결하는 단계; (b)상기 은행이 제공하는 콘텐츠를 상기 보안 단문 메시지 서버를 통해 암호화된 상태로 이동통신 사업자의 단문 메시지 센터를 통해 무선단말기로 전송하는 단계; 및 (c)상기 무선단말기로 상기 보안 단문 메시지 서버에서 전송 받은 데이터를 복호화하는 단계를 포함함을 특징으로 한다.

이하 도면을 참조하여 본 발명을 상세히 설명하기로 한다.

도 3은 본 발명에 의한 CDMA네트워크 상의 양방향 단문메시지 서비스에서 사용자 패스워드를 이용한 상호 인증 및 보안 서비스 구성을 도시한 것으로, 보안 메시지(SSMS) 서버(300), 메시지 송신기(310), 데이터 네트워크(320), 메시지 센터(330), 셀룰라 스위치(340), 기지국(350) 및 이동통신단말기(360)로 이루어진다.

도 4는 본 발명에 의한 CDMA네트워크 상의 양방향 단문메시지 서비스에서 사용자 패스워드를 이용한 상호 인증 및 보안 서비스에 대한 프로토콜 계층도를 도시한 것이다.

본 발명에 의한 단문메시지 서비스의 프로토콜은 크게 보안 단문메시지 서비스(SSMS) 계층, 단문메시지 서비스 텔레서비스 계층, 단문 메시지 서비스 전송 계층 및 단문메시지 서비스 릴레이 계층 4계층으로 이루어져 있다.

링크계층은 EIA/TIA/IS-95A를 사용하여 기지국(350)은 이동통신단말기(360)와 메시지 센터(330)과 연결하고 있으며, 또한 메시지 센터(330)는 보안 단문메시지 서비스 서버(300)와 연결하고 있다. 단문메시지 서비스 전송계층과 릴레이 계층은 실제 메시지 센터(330)와 단대단으로 연결될 필요는 없으나 단문메시지 서비스의 텔레서비스 계층은 메시지 센터(330)와 단대단으로 연결되어야 한다. 따라서 기지국(350)과 메시지 센터(330)와는 유선망으로 연결되어 전송계층까지는 EIA/TIA/IS-95A와 그 상위 단문메시지 서비스 전송계층과 릴레이 계층을 통해서 연결된다.

본 발명에서는 사용자의 패스워드만을 이용하여 상호인증과 보안을 제공하는 것으로, 사용자의 패스워드는 각 콘텐츠 제공자마다 다르게 관리된다.

따라서, SSMS 서버(300)는 우선 사용자 식별번호와 패스워드를 가지고 임시키를 만들고 세션키 생성에 사용될 난수를 발생시킨 다음 이것을 임시 키로 암호화하여 이동통신단말기(360)에 전송한다.

이동통신단말기(360) 사용자는 자신의 패스워드를 입력하여 임시키를 생성한 다음 복호화하여 난수를 재생한다.

이 재생된 난수를 가지고 서버(300)와 이동통신단말기(360)는 각각 두 번째 임시키를 만들어 challenge-response 프로토콜의 파라미터 암호화 및 복호화에 사용한다.

최종적으로 만들어지는 세션키는 앞의 두 키와 SSMS 서버(300)와 생성하는 두 번째 난수까지 포함하여 생성되며 이후 모든 사용자 데이터는 이 세션키로 암호화 및 복호화가 이루어진다.

이 세션키의 생명은 하나의 세션 혹은 트랜잭션으로 제한되어 그 세션이 끝나거나 연결이 끊어지며 또 다른 세션키를 생성해야 한다.

세션키 생성과정에서 두 개의 난수가 사용됨으로써 세션키의 난수성을 보장하고 있으며 Brute-Force 공격과 오프라인 Dictionary 공격을 방지하고 있다.

1. 양방향 보안 단문메시지의 메시지 헤더 구성은 다음과 같다.

Message := {

UCHAR8 MSG_HDR;

UCHAR8 SSN_HDR (3);

UCHAR8 DATA_LEN(2);

UCHAR8 DATA(32..60);

UCHAR8 MAC(8);

}

MSG_HDR := MSG_TYPE | VERSION;

MSG_TYPE

정의: 메시지 형식

길이: 4bits

인코딩: 1000 - 암호화된 단방향 단문 메시지

1001 - 암호화된 양방향 단문 메시지

0000 - 평문 단방향 단문 메시지

0001 - 평문 양방향 단문 메시지

VERSION

정의: 프로토콜의 현재버전

길이: 4bits

인코딩: 처음 두자리는 주버전(MAIN VERSION), 다음 두자리는 부버 전(SUB VERSION)이다. 즉, 1.1이면 0101이 된다.

SSN - HDR := {

UCHAR8 SSN_INFO(2);

UCHAR8 MSG_FRAG;

}

SSN_INFO :=SSN_ID | SEQ_NO

SSN_ID

정의: 각각의 세션 식별 번호

길이: 8bit

SEQ_NO

정의: 각 세션에서 메시지 시퀀스 번호

길이: 8bit

MSG_FRAG:=FLAG | FSEQ_NO

FLAG

정의: 팻킷 단편화 플래그

길이: 1bit

인코딩: 0 - 단편화되어 있지 않음

1

MSG_LEN

정의: 각 단문 메시지의 길이

길이: 16bit

인코딩: little - endian

DATA

정의: 암호화된 메시지

길이: 가변(최대길이는 약 480 비트 정도이다.)

MAC

정의: 메시지 인증 코드. 이 메시지 인증코드는 원문을 단방향 해쉬 함수를 적용하여 나온 값의 왼쪽 64 비트와 오른쪽 64비트를 XOR 하여 나온 값을 사용하도록 한다.

길이: 64bit

2. 양방향 보안 단문 메시지의 사용자 패스워드를 통한 양방향 인증 및 키 교환 프로토콜은 다음과 같다.

2.1 제한 요건

최대 메시지 길이: 40 bytes(Plaintext message with 7bit encoding)

다른 제한 요건은 단방향의 경우와 같다.

2.2 용어정의

ID_{user} : 콘텐츠 제공자별 사용자 식별번호, 8byte

PW_{user} : 콘텐츠 제공자별 사용자 비밀번호, 8byte

r_1 : 공유 비밀키 생성에 사용되는 난수, 8byte

r_2 : 공유 비밀키 생성에 사용되는 난수, 8byte

C_1 : SSMS에서 MS로 보내는 랜덤 챌린지, 16byte

C_2 : MS에서 SSMS로 보내는 랜덤 챌린지, 16byte

K_1 : 첫 번째 유추된 공유 비밀키, 16byte

K_2 : 두 번째 유추된 공유 비밀키, 16byte

K_s : 공유 비밀키, 16byte

IV: 초기벡터, 16byte

2.3 공유 비밀키 생성 프로세스

$K_1 : f_1 (h(ID_{user}), h(PW_{user}), h(ID_{CP}), PRNG(h(r_1), h(PW_{user})))$

$K_2 : f_2 (PRNG(h(r_2), h(PW_{user})), K_1, h(ID_{user}), h(PW_{user}))$

$K_s : f_3 (K_1, K_2, h(PW_{user}))$

2.3.1 키 생성 프로세스

단방향과 양방향 서비스 모두 같은 키 유추 함수를 사용하고 있으나 단방향의 경우 f_3 만 사용하고 있고 양방향의 경우 모두 사용한다.

키 유추 함수들은 기본적으로 다단계 암호화 기법에 근거하여 정의되었으며 각 함수의 결과 값들은 특정한 시퀀스가 생기지 않도록 하였다.

우선 각각의 함수의 정의는 다음과 같다.

$K_1 : f_1 (X_1, X_2, X_3, X_4)$

$K_2 : f_2 (X_1, X_2, X_3, X_4)$

$K_s : f_3 (X_1, X_2, X_3)$

정의 : $f_1 (X_1, X_2, X_3, X_4)$

$y = f_1 (X_1, X_2, X_3, X_4) = PRNG(h(PRNG(h(PRNG(X_1, X_4)), X_3)), X_2)$

정의 : $f_2 (X_1, X_2, X_3, X_4)$

$y = f_2 (X_1, X_2, X_3, X_4) = PRNG(h(PRNG(h(PRNG(X_1, X_2), X_3)), X_4)$

정의 : $f_3 (X_1, X_2, X_3)$

$y = f_3 (X_1, X_2, X_3) = PRNG(h(PRNG(X_3, X_2), X_1)$

이 각각의 함수들은 모두 난수 발생기에 근거하고 있으나 난수 발생기가 가단계 암호화 기법에 근거하고 있으며 각 함수의 파라미터의 순서는 공개된 정보와 비공개된 정보, 유추된 정보의 세가지 군으로 나누어서 보안성을 고려하여 정해졌다. 이 함수들은 결과 값들의 시퀀스만 예측이 불가능하고 각각의 파라미터 개수만 일치하면 임의대로 정의할 수 있다.

또한, 본 발명에 의한 구체적인 실시예라고 할 수 있는 무선뱅킹시스템에 대하여 설명하기로 한다.

무선뱅킹시스템을 구축하기 위해서는 우선 이동통신사업자와 은행, 그리고 무선단말기 사업자가 동시에 참여해야한다.

이동통신 사업자는 은행과 전용선 등을 통해 자신의 단문 메시지 센터와 은행의 보안 단문 메시지 서버 사이의 연결을 제공한다.

은행은 콘텐츠 제공자로서 자신의 콘텐츠를 보안 단문 메시지 서버를 통해 암호화된 상태로 이동통신 사업자의 단문 메시지 센터를 통해 무선 단말기로 전송한다. 무선단말기 사업자는 자신의 무선단말기의 소프트웨어를 업그레이드하여 보안 단문 메시지 서비스를 가능하도록 한다.

업그레이드가 된 무선 단말기는 보안 단문 메시지 서비에서 전송받은 데이터를 복호화할 수 있다.

도면과 명세서는 단지 본 발명의 예시적인 것으로서, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

발명의 효과

본 발명에 의하면, 기존의 보안성 없는 단문메시지 서비스로는 불가능했던 다양한 서비스들이 제공 가능해진다.

이는 기존의 무선 인터넷폰에서만 가능했던 서비스들을 기존의 구형단말기들에서도 가능하게 해준다. 예를 들어 무선 인터넷폰 기종이 부가되지 않은 기존의 구형 단말기들은 간단한 소프트웨어 업그레이드를 통해서 무선 금융 거래나 증권거래 등의 서비스를 제공받을 수 있다.

(57) 청구의 범위

청구항 1.

(a)사용자 식별번호와 패스워드를 가지고 임시키를 만들고, 세션키 생성에 사용될 난수를 발생시키고, 상기 난수를 임시키로 암호화하여 무선단말기에 전송하는 단계;

(b)상기 무선단말기에 사용자의 패스워드를 입력하여 임시키를 생성한 다음 복호화하여 난수를 재생하는 단계;

(c)상기 재생된 난수를 가지고 상기 서버와 상기 무선단말기는 각각 두 번째 임시키를 만드는 단계;

(d)상기 두 임시키와 상기 서버에서 생성하는 두 번째 난수까지 포함하여 세션키를 생성하는 단계; 및

(e)상기 세션키를 이용하여 암호화 및 복호화하는 단계를 포함함을 특징으로 하는 양방향 단문메시지 서비스에서 사용자 패스워드를 이용한 상호인증 및 보안방법.

청구항 2.

제1항에 있어서, 상기 세션키는

하나의 세션 또는 트랜잭션으로 제한되어 그 세션이 끝나거나 연결이 끊어지며 또 다른 세션키를 생성함을 특징으로 하는 양방향 단문메시지 서비스에서 사용자 패스워드를 이용한 상호인증 및 보안방법.

청구항 3.

제1항에 있어서, 상기 세션키는

생성과정에서 두 개의 난수가 사용됨으로써 세션키의 난수성을 보장하고 있으며 Brute-Force 공격과 오프라인 Dictionary 공격을 방지함을 특징으로 하는 양방향 단문메시지 서비스에서 사용자 패스워드를 이용한 상호인증 및 보안방법.

청구항 4.

단문메시지 서비스를 이용한 무선뱅킹서비스 방법에 있어서,

(a)이동통신 사업자의 단문 메시지 센터와 은행의 보안 단문 메시지 서버를 연결하는 단계;

(b)상기 은행이 제공하는 콘텐츠를 상기 보안 단문 메시지 서버를 통해 암호화된 상태로 이동통신 사업자의 단문 메시지 센터를 통해 무선단말기로 전송하는 단계; 및

(c)상기 무선단말기로 상기 보안 단문 메시지 서버에서 전송 받은 데이터를 복호화하는 단계를 포함함을 특징으로 하는 양방향 단문메시지 서비스를 이용한 무선뱅킹서비스 방법.

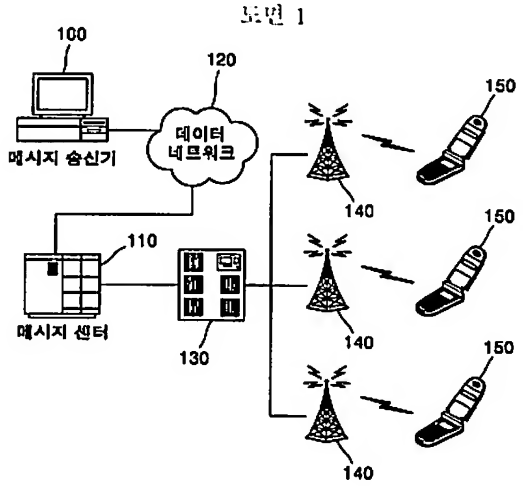
청구항 5.

제4항에 있어서, 상기 (c)단계는

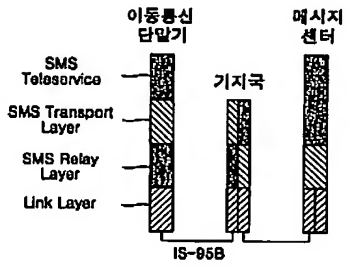
상기 무선단말기 사업자가 제공하는 무선단말기의 소프트웨어를 보안 단문 메시지 서비스가 가능하도록 업그레이드하는 단계를 더 구비함을 특징으로 하는 양방향 단문메시지 서비스를 이용한 무선뱅킹서비스 방법.

도면

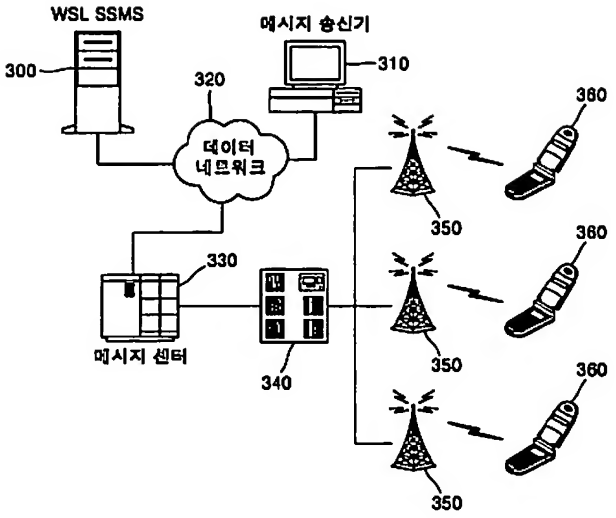
도면 1



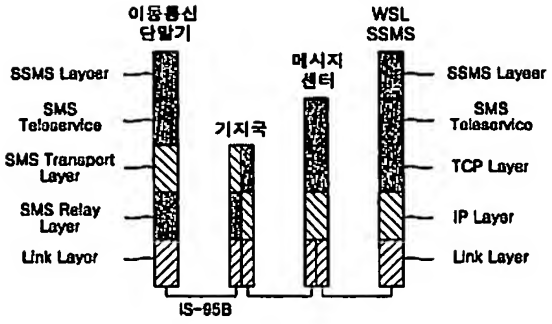
도면 2



도면 3


WSL SSMS
300
메시지 송신기
310
320
데이터 네트워크
360
350
360
330
메시지 센터
340
350
360
350

도면 4


이동통신 단말기
WSL SSMS
SSMS Layer
SMS Teleservice
SMS Transport Layer
SMS Relay Layer
Link Layer
기지국
메시지 센터
SSMS Layer
SMS Teleservice
TCP Layer
IP Layer
Link Layer
IS-95B